NS3 as Test Bed Environment for Botnet Studies

Braden Soper [†], Jim Brase* and Ryan Prenger*

[†] University of California, Santa Cruz
beesoap@soe.ucsc.edu

*Lawrence Livermore National Laboratory
brase1@llnl.gov, prenger1@llnl.gov

MOTIVATION

- Prediction, detection and control of botnets is of significant value to network defenders.
- However, controlled experiments of botnets are not feasible due to their distributed nature, legal/privacy issues and security risks.
- NS3 is an open-source, discrete event based network simulator software package.
- We explore NS3 as a virtual test bed for studying botnets.
- The problem of finding an optimal timing strategy for a DDoS attack is used as a preliminary case study

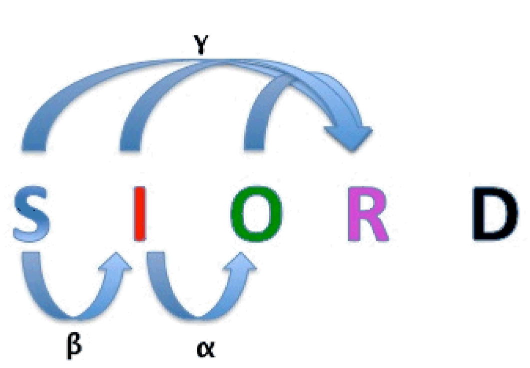
ANALYTIC MODEL

Consider a compartmental epidemiological model with state variables S (susceptible), I (Infected), O (owned), R (recovered) and D (dead). Assume the network is fixed with N total computers. At time t_a the botmaster launches a DDoS attack on the network.

Parameters	Initial Conditions
α : owning rate	$S(0) = N - 1$
β : infection rate	$I(0) = 1$
γ : patch rate	$O(0) = 0$
A : attack rate	$R(0) = 0$
$\mathbb{1}_{\{\}}$: indicator function	$D(0) = 0$
t_a : DDoS attack time	

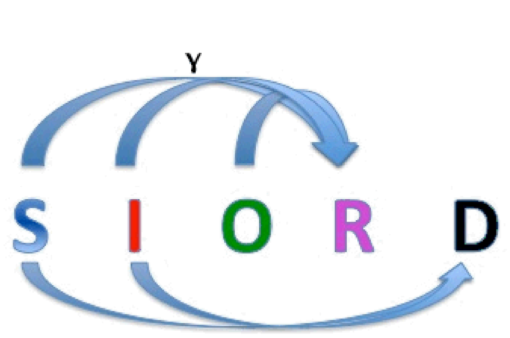
State Equations for $t \in [0, t_a)$

$$\dot{S} = -\beta SI - \gamma S$$
$$\dot{I} = \beta SI - (\alpha + \gamma) I$$
$$\dot{O} = \alpha I - \gamma O$$
$$\dot{R} = \gamma (S + I + O)$$
$$\dot{D} = 0$$



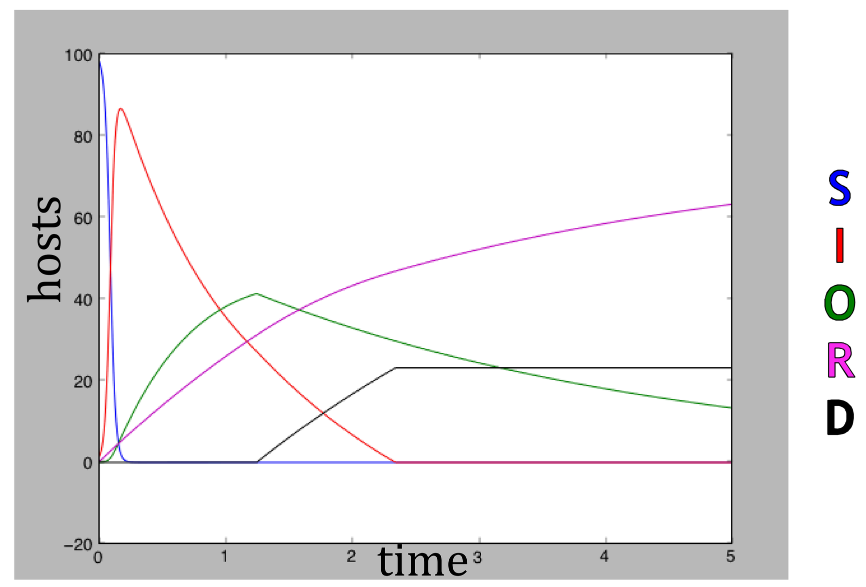
State Equations for $t \in [t_a, \infty)$

$$\dot{S} = -AO\mathbb{1}_{\{S>0\}} - \gamma S$$
$$\dot{I} = -AO\mathbb{1}_{\{I>0\}} - \gamma I$$
$$\dot{O} = -\gamma O$$
$$\dot{R} = \gamma (S + I + O)$$
$$\dot{D} = AO(\mathbb{1}_{\{S>0\}} + \mathbb{1}_{\{I>0\}})$$



NUMERICAL RESULTS FOR ANALYTIC MODEL

Given parameter values Runge-Kutta methods can be used to find solutions to the analytical model.



$N = 100, \alpha = 0.8, \beta = 50/N, \gamma = 0.3, A = 0.6, t_a = 1.25$

Steady State as t → ∞

$$(S, I, O, R, D) \to (0, 0, 0, R^*, D^*)$$

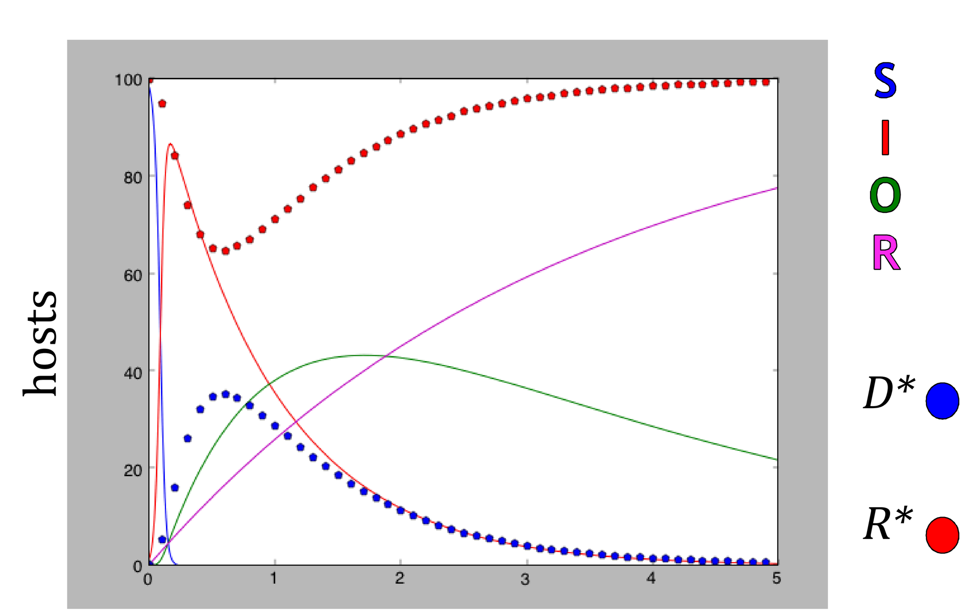
$$D^* = \lim_{t \to \infty} D(t) \quad \text{and} \quad R^* = \lim_{t \to \infty} R(t)$$

- Different values of t_a will result in different values of D^* and R^*.
- Thus we can consider D^* and R^* to be functions of t_a.
- The optimal DDoS attack time for the botmaster is given as follows.

Optimal DDoS Launch Time

$$T_a = \arg\max_{t_a > 0} D^*(t_a)$$

Runge-Kutta methods can again be used to find T_a. The following plot shows final values of D* and R* over time. Results are plotted over SIOR dynamics.

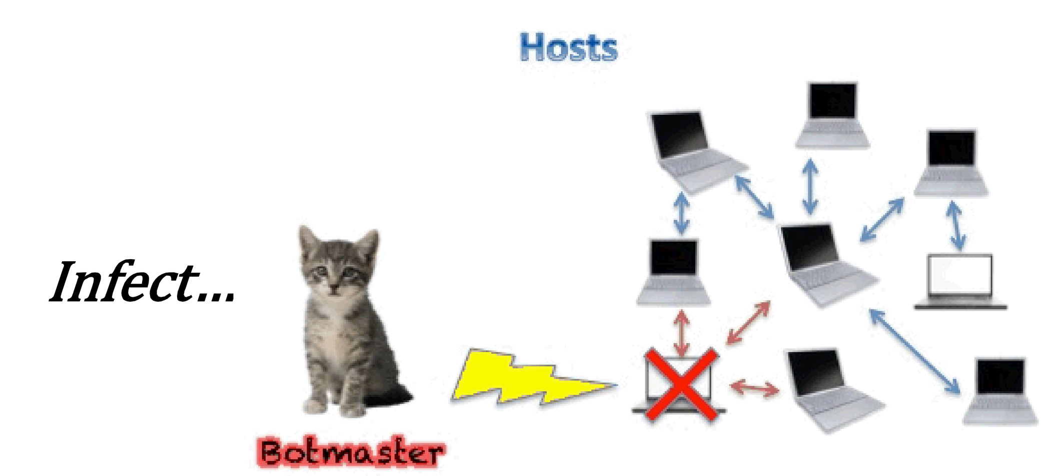


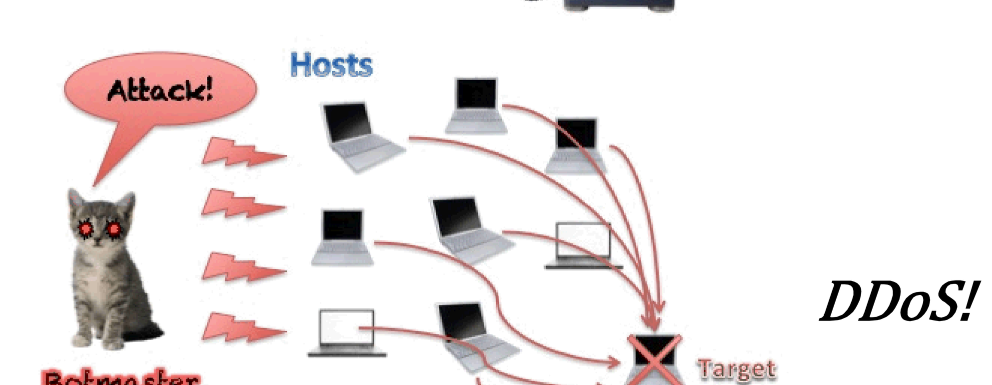
NS3 SIMULATION

- The simulation environment was created in Python
- Host, Defender and Botmaster agents were defined as Python classes.
- The NS3 event-scheduler was used to run the simulation.

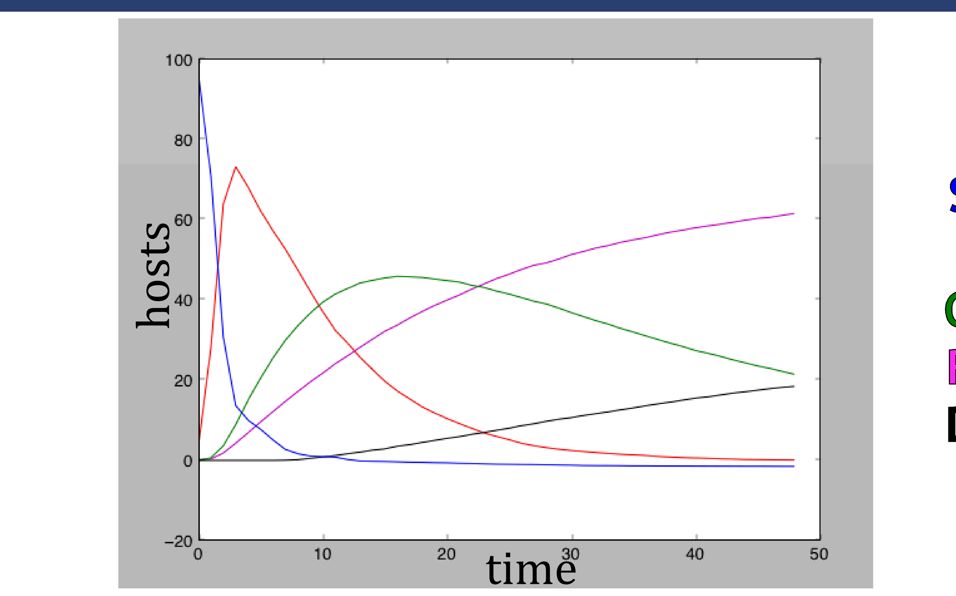
NS3 Agents

Basic Agents Behavior

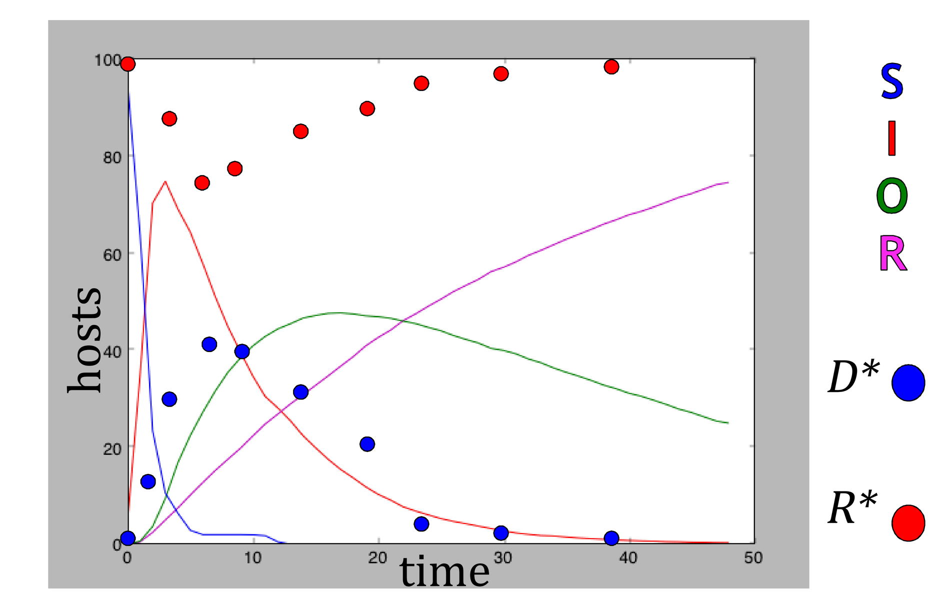




NS3 SIMULATION RESULTS



$N = 100, \alpha = 0.8, \beta = 50/N, \gamma = 0.3, A = 0.6, t_a = 1.25$



CONCLUSIONS & FUTURE WORK

NS3 appears to provide a suitable environment for testing botnet dynamics. We were able to show this by finding the optimal DDoS launch time for a botnet. NS3 simulation results and theoretical predictions matched reasonably well. Future work within the NS3 environment includes the following.

- Define multiple botmaster agents to study the interaction between botnets competing for scarce resources.
- Define multiple host agents with varying characteristics (i.e. bandwidth, memory, processors, etc.).
- Define multiple defender agents tasked with guarding certain subsets of the host agents.
- Compare game theoretic predictions against NS3 simulations results.
- Explore the existence of Nash Equilibrium in Attacker vs. Defender games.
- Explore the existence of Evolutionary Stable Strategies in Botnet vs. Botnet games.
- Compare NS3 simulations against real-world data.
- Test botnet detection methodologies within the NS3 environment.

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract No. DE-AC52-07NA27344

LLNL - POST-571237